WHAT IS CLAIMED IS:

1. A digital signature system comprising a center computer and a first and second terminal devices which can communicate with each other, wherein:

the center computer generates and outputs a signing-key to be inputted in the first terminal device, and generates and outputs a verification-key to be inputted in the second terminal device;

the first terminal device accepts the signing-key, generates a digital signature for a digital data to be signed using the signing-key, and outputs the digital signature to be inputted in the second terminal device; and

the second terminal device accepts the verification-key, the signer's identity, the identification code of the digital data and the digital signature, and verifies the validity of the digital signature using the verification-key, the signer's identification code and the identification code of the digital data.

2. The digital signature system according to claim 1, wherein the center computer comprises:

a first generating means for generating the signing-key for the signer;

a second generating means for generating the verification-key for the verifier;

a first output device outputting the signing-key generated by the first generating means; and

a second output device outputting the verification-

key generated by the second generating means.

3. The digital signature system according to claim 1, wherein the first terminal device capable of communicating with the center comprises:

an accepting means for accepting the signer's signing-key;

a first input device inputting the signer's signing-key;

a second input device inputting the identification code of the digital data;

a third generating means for generating the digital signature; and

a third output device outputting the digital signature generated by the generating means.

4. The digital signature system according to claim 1, wherein the second terminal device capable of communicating with the center comprises:

a first accepting means for the verification-key;

a third input device inputting the verifier's verification-key;

a second accepting means for accepting the signer's identity;

a fourth input device inputting the signer's identification code;

a third accepting means for the identification code of the digital data;

a fifth input device inputting the identification code

of the digital data;

a fourth accepting means for accepting the digital signature;

a sixth input device inputting the digital signature;

a verifying means for verifying the validity of the digital signature using the verification-key, the signer's identification code and the identification code of the digital data; and

a fourth output device outputting the result of verifying the validity of the digital signature, namely, acceptable as valid or not.

5. A method, in a digital signature system comprising a center computer and a first and second terminal devices which can communicate with each other, comprising the steps of:

in the center computer, generating and outputting a signing-key to be inputted in the first terminal device, and generating and outputting a verification-key to be inputted in the second terminal device;

in the first terminal device, inputting the signing-key, generating a digital signature for a digital data to be signed using the signing-key, and outputting the digital signature to be inputted in the second terminal device; and

in the second terminal device, inputting the verification-key, the signer's identification code, the identification code of the digital data and the digital signature, and verifying the validity of the digital

signature using the verification-key, the signer's identification code and the identification code of the digital data.

6. The method according to claim 5 further comprising the steps of: in the center computer,

generating the signing-key for the signer;

generating the verification-key for the verifier;

outputting the generated signing-key; and

outputting the generated verification-key.

7. The method according to claim 5 further comprising the steps of: in the first terminal device,

inputting the signer's signing-key;

inputting the identification code of the digital data;

generating the digital signature; and

outputting the generated digital signature.

8. The method according to claim 5 further comprising the steps of: in the second terminal device,

inputting the verifier's verification-key;

inputting the signer's identification code;

inputting the identification code of the digital data;

inputting the digital signature;

outputting the result of verifying the validity of the digital signature, namely, acceptable as valid or not.

9. A computer readable recording medium having a first, second and third programs recorded thereon,

the first program controlling a center computer so as to generate and output a signing-key to be inputted in

a first terminal device, to generate and output a verification-key to be inputted in a second terminal device;

the second program controlling the first terminal device so as to accept the signing-key, to generate a digital signature for a digital data to be signed using the signing-key, and to output the digital signature to be inputted in the second terminal device; and

the third program controlling the second terminal device so as to accept the verification-key, the signer's identity, the identification code of the digital data and the digital signature, and to verify the validity of the digital signature using the verification-key, the signer's identification code and the identification code of the digital data.

10. The computer readable recording medium according to claim 9, wherein the first program controls the center computer so as to:

generate the signing-key for the signer;

generate the verification-key for the verifier;

output the generated signing-key; and

output the generated verification-key.

11. The computer readable recording medium according to claim 9, wherein the second program controls the first terminal device so as to:

accept the signer's signing-key;

input the signer's signing-key;

input the identification code of the digital data;

generate the digital signature; and

output the generated digital signature.

12. The computer readable recording medium according to claim 9, wherein the third program controls the second terminal device so as to:

accept the verification-key;

input the verifier's verification-key;

accept the signer's identity;

input the signer's identification code;

accept the identification code of the digital data;

input the identification code of the digital data;

accept the digital signature;

input the digital signature;

verify the validity of the digital signature using the verification-key, the signer's identification code and the identification code of the digital data; and

output the result of verifying the validity of the digital signature, namely, acceptable as valid or not.

13. A center computer in a digital signature system comprising:

a first generating means for generating a signing-key for a signer;

a second generating means for generating a verification-key for a verifier;

a first output device outputting the signing-key generated by the first generating means; and

a second output device outputting the verification-key generated by the second generating means.

14. The center computer, according to claim 13, wherein:

the first generating means comprises means for generating a first multivariate function, and means for generating a second multivariate function obtained by substituting the signer's identification code into a first variable of the first multivariate function;

the first output device outputs the second multivariate function as the signing-key for the signer;

the second generating means comprises means for generating a random number, a third multivariate function obtained by substituting the random number to a second variable of the first multivariate function; and

the second output device outputs the random number and the third multivariate function as the verification-key for the verifier.

15. The center computer according to claim 14, wherein:

the second multivariate function is generated by substituting the signer's identification code into a first group of variables of the first multivariate function.

16. The center computer according to claim 14, wherein:

a group of random numbers is generated and the third multivariate function is generated by substituting

the group of random numbers into a second group of variables of the first multivariate function; and

the group of random numbers and the third multivariate function are outputted as the verification-key for the verifier.

17. A method of establishing a signing-key for a signer and a verification-key for a verifier comprising the steps of:

generating a first multivariate function;

generating a second multivariate function obtained by substituting the signer's identification code into a first variable of the first multivariate function;

outputting the second multivariate function as a signing-key for the signer;

generating a random number, a third multivariate function obtained by substituting the random number into a second variable of the first multivariate function; and

outputting the random number and the third multivariate function as a verification-key for the verifier.

18. The method of establishing a signing-key according to claim 17, wherein:

the second multivariate function is generated by substituting the signer's identification code into a first group of variables of the first multivariate function; and

the second multivariate function is outputted as a signing-key for the signer.

19. The method of establishing a verification-key

according to claim 17, wherein:

a group of random numbers is generated and the third multivariate function is generated by substituting the group of random numbers into a second group of variables of the first multivariate function; and

the group of random numbers and the third multivariate function are outputted as a verification-key for the verifier.

20. A computer readable recording medium having a program recorded thereon, the program controlling the computer so as to:

generate a first multivariate function;

generate a second multivariate function obtained by substituting a signer's identification code into a first variable of the first multivariate function;

output the second multivariate function as a signing-key for the signer;

generate a random number, a third multivariate function obtained by substituting the random number to a second variable of the first multivariate function; and

output the random number and the third multivariate function as a verification-key for the verifier.

21. The computer readable recording medium according to claim 20, wherein the program controls the computer so as to:

generate the second multivariate function by substituting the signer's identification code into a first

group of variables of the first multivariate function; and

output the second multivariate function as a signing-key for the signer.

22. The computer readable recording medium according to claim 20, wherein the program controls the computer so as to:

generate a group of random numbers and generate a third multivariate function by substituting the group of random numbers into a second group of variables of the first multivariate function; and

output the group of random numbers and the third multivariate function as a verification-key for the verifier.

23. A method of establishing a digital signature in a digital signature system comprising a center computer and a first and second terminal devices which can communicate with each other, comprising the steps of:

in the center computer,

generating a first multivariate function,

generating a second multivariate function obtained by substituting a signer's identification code into a first variable of the first multivariate function,

outputting the second multivariate function as a signing-key for the signer,

generating a random number, a third multivariate function obtained by substituting the random number into a second variable of the first multivariate function, and

outputting the random number and the third

multivariate function as a verification-key for a verifier;

in the first terminal device,

accepting the signer's signing-key;

inputting the accepted signer's signing-key;

inputting an identification code of a digital data;

generating a fourth multivariate function obtained by substituting the identification code of the digital data into the third variable of the second multivariate function, and

outputting the fourth multivariate function as a digital signature;

in the second terminal device,

accepting the verification-key,

inputting the accepted verifier's verification-key,

accepting the signer's identity,

inputting the signer's identification code,

accepting the identification code of the digital data,

inputting the accepted identification code of the digital data,

accepting the digital signature,

inputting the accepted digital signature,

generating a first evaluation value by substituting the random number into the second variable of the fourth multivariate function,

generating a second evaluation value by substituting the signer's identification code and the identification code of the digital data into the first and

third variables of the third multivariate function, respectively, and

accepting the digital signature as valid if both of the first and second evaluation values equal, and otherwise rejecting the digital signature as invalid.

24. A first terminal device in a digital signature system comprising:

an accepting means for accepting a signer's signing-key;

a first input device inputting the signer's signing-key;

a second input device inputting an identification code of a digital data;

a generating means for generating a digital signature; and

an output device outputting the digital signature generated by the generating means.

25. The first terminal device according to claims 24, wherein:

the digital signature generating means generates a fourth multivariate function obtained by substituting an identification code of a digital data into a third variable of a second multivariate function; and

the output device outputs the fourth multivariate function as the digital signature.

26. The first terminal device according to claim 25, wherein:

the digital signature generating means generates a fourth multivariate function by substituting an identification code of a digital data into a third group of variables of a second multivariate function; and

the output device outputs the fourth multivariate function as the digital signature.

27. A method of establishing a digital signature comprising the steps of:

accepting a signer's signing-key;

inputting the accepted signer's signing-key;

inputting an identification code of a digital data;

generating a fourth multivariate function obtained by substituting the identification code of the digital data into a third variable of a second multivariate function; and

outputting the fourth multivariate function as a digital signature.

28. The method of establishing a digital signature according to claims 27, wherein:

a fourth multivariate function is generated by substituting an identification code of a digital data into a third group of variables of a second multivariate function; and

the fourth multivariate function is outputted as a digital signature.

29. A computer readable recording medium having a program recorded thereon, the program controlling a computer so as to:

accept an inputted signer's signing-key;

accept an inputted identification code of a digital data;

generate a fourth multivariate function obtained by substituting the identification code of the digital data into a third variable of a second multivariate function; and

output the fourth multivariate function as a digital signature.

30. The computer readable recording medium according to claim 29, wherein the program controls the computer so as to:

generate a fourth multivariate function by substituting an identification code of a digital data into a third group of variables of a second multivariate function; and

output the fourth multivariate function as a digital signature.

31. A second terminal device in a digital signature system comprising:

a first accepting means for accepting a verification-key;

a first input device inputting the verifier's verification-key;

a second accepting means for accepting a signer's identity;

a second input device inputting the signer's identification code;

a third accepting means for an identification code of a digital data;

a third input device inputting the identification code of the digital data;

a fourth accepting means for accepting a digital signature;

a fourth input device inputting the digital signature;

a verifying means for verifying the validity of the digital signature using the verification-key, the signer's identification code and the identification code of the digital data;

an output device outputting the result of verifying the validity of the digital signature, namely, acceptable as valid or not.

32. The second terminal device according to claim 31, wherein the verifying means for verifying the validity of the digital signature:

generates a first evaluation value by substituting a random number into a second variable of a fourth multivariate function;

generates a second evaluation value by substituting the signer's identification code and the identification code of the digital data into a first and third variables of a third multivariate function, respectively; and

accepts the digital signature as valid if both of the first and second evaluation values equal, and otherwise

rejects the digital signature as invalid.

33. The second terminal device according to claim 32, wherein a first evaluation value is generated by substituting a group of random numbers into a second group of variables of the fourth multivariate function.

34. The second terminal device according to claim 32, wherein the signer's identification code is substituted into a first group of variables of the third multivariate function, or the identification code of the digital data is substituted into a third group of variables of the third multivariate function.

35. A method of verifying the validity of a digital signature comprising the steps of:

accepting a verifier's verification-key;

inputting the accepted verification-key;

accepting a signer's identity;

inputting the signer's identification code;

accepting an identification code of a digital data;

inputting the identification code of the digital data;

accepting a digital signature;

inputting the digital signature;

generating a first evaluation value by substituting a random number into a second variable of a fourth multivariate function;

generating a second evaluation value by substituting the signer's identification code and the identification code of the digital data into a first and third

variables of a third multivariate function, respectively; and

accepting the digital signature as valid if both of the first and second evaluation values equal, and otherwise rejecting the digital signature as invalid.

36. The method of verifying the validity of a digital signature according to claim 35, wherein a first evaluation value is generated by substituting a group of random numbers into a second group of variables of the fourth multivariate function.

37. The method of verifying the validity of a digital signature according to claim 35, wherein the signer's identification code is substituted into a first group of variables of the third multivariate function, or the identification code of the digital data is substituted into a third group of variables of the third multivariate function.

38. A computer readable recording medium having a program recorded thereon, the program controlling the computer so as to:

accept an inputted verifier's verification-key;

accept an inputted signer's identification code;

accept an inputted identification code of a digital data;

accept an inputted digital signature;

generate a first evaluation value by substituting a random number into a second variable of a fourth multivariate function;

generate a second evaluation value by substituting the signer's identification code and the identification code of the digital data into a first and third variables of a third multivariate function, respectively; and

accept the digital signature as valid if both of the first and second evaluation values equal, and otherwise reject the digital signature as invalid.

39. The computer readable recording medium according to claim 38, wherein the program controls the computer so as to generate a first evaluation value by substituting a group of random numbers into a second group of variables of the fourth multivariate function.

40. The computer readable recording medium according to claim 38, wherein the program controls the computer so as to substitute the signer's identification code into a first group of variables of the third multivariate function, or substitute the identification code of the digital data into a third group of variables of the third multivariate function.

41. The center computer, according to claim 14, in which a multivariate polynomial over a finite field is used for a multivariate function.

42. The method according to claim 17, in which a multivariate polynomial over a finite field is used for a multivariate function.

43. The computer readable recording medium according to claim 20, in which a multivariate polynomial

over a finite field is used for a multivariate function.

44. The first terminal device, according to claim 25, in which a multivariate polynomial over a finite field is used for a multivariate function.

45. The method according to claim 27, in which a multivariate polynomial over a finite field is used for a multivariate function.

46. The computer readable recording medium according to claim 29, in which a multivariate polynomial over a finite field is used for a multivariate function.

47. The second terminal device, according to claim 32, in which a multivariate polynomial over a finite field is used for a multivariate function.

48. The method according to claim 35, in which a multivariate polynomial over a finite field is used for a multivariate function.

49. The computer readable recording medium according to claim 38, in which a multivariate polynomial over a finite field is used for a multivariate function.

50. The center computer according to claim41, in the generating means for the first multivariate function, a multivariate polynomial over a finite field is selected uniformly at random by selecting each coefficient of the polynomial uniformly at random from the finite field.

51. The method according to claim 42, in which a multivariate polynomial over a finite field is selected uniformly at random by selecting each coefficient of the

polynomial uniformly at random from the finite field.

52. The computer readable recording medium according to claim 43, in which a multivariate polynomial over a finite field is selected uniformly at random by selecting each coefficient of the polynomial uniformly at random from the finite field.

53. The center computer according to claim 41, in which a maximum degree of the first variable in the multivariate polynomial is taken more than or equal to n-1, where n is the number of signers.

54. The method according to claim 42, in which a maximum degree of the first variable in the multivariate polynomial is taken more than or equal to n-1, where n is the number of signers.

55. The computer readable recording medium according to claim 43, in which a maximum degree of the first variable in the multivariate polynomial is taken more than or equal to n-1, where n is the number of signers.

56. The center computer according to claim 41, in which the number of the second variable in the multivariate polynomial is taken more than or equal to a pre-defined number of colluders among verifiers.

57. The method according to claim 42, in which the number of the second variable in the multivariate polynomial is taken more than or equal to a pre-defined number of colluders among verifiers.

58. The medium according to claim 43, in which the

number of the second variable in the multivariate polynomial is taken more than or equal to a pre-defined number of colluders among verifiers.

59. The center computer according to claim 41, in which a maximum degree of the third variable in the multivariate polynomial is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

60. The method according to claim 42, in which a maximum degree of the third variable in the multivariate polynomial is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

61. The medium according to claim 43, in which a maximum degree of the third variable in the multivariate polynomial is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

62. The system according to claim 1, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

63. The method according to claim 5, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

64. The medium according to claim 9, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

65. The first terminal device according to claim 24, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

66. The method according to claim 27, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

67. The computer readable medium according to claim 29, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

68. The second terminal device according to claim 31, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

69. The method according to claim 35, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

70. The computer readable recording medium according to claim 38, in which the identification code of a digital data is a compressed data or an encoded data of a digital data by a hash function.

71. The first terminal device according to claim 44, in which a maximum degree of the third variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

72. The method according to claim 45, in which a maximum degree of the third variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

73. The computer readable medium according to claim 46, in which a maximum degree of the third variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

74. The second terminal device according to claim 47, in which the number of the second variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number of colluders among verifiers.

75. The method according to claim 48, in which the number of the second variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number of colluders among verifiers.

76. The computer readable recording medium according to claim 49, in which the number of the second variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number of colluders among verifiers.

77. The second terminal device according to claim47, in which a maximum degree of the first variable in the multivariate polynomial over a finite field is taken more

than or equal to n-1, where n is the number of signers.

78. The method according to claim 48, in which a maximum degree of the first variable in the multivariate polynomial over a finite field is taken more than or equal to n-1, where n is the number of signers.

79. The computer readable recording medium according to claim 49, in which a maximum degree of the first variable in the multivariate polynomial over a finite field is taken more than or equal to n-1, where n is the number of signers.

80. The second terminal device according to claim 47, in which a maximum degree of the third variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

81. The method according to claim 48, in which a maximum degree of the third variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.

82. The computer readable recording medium according to claim 49, in which a maximum degree of the third variable in the multivariate polynomial over a finite field is taken more than or equal to a pre-defined number up to which each signer is allowed to generate digital signatures.